PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-187013
(43)Date of publication of application : 09.07.1999

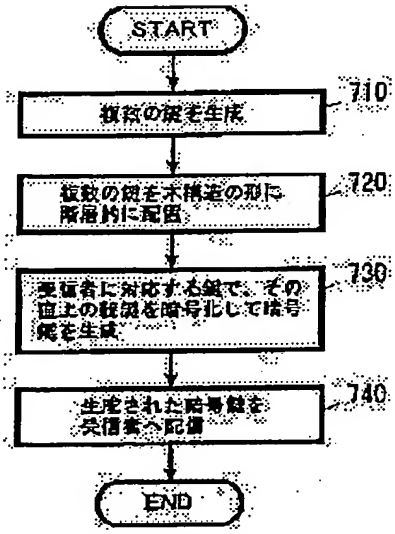
(51)Int.Cl. H04L 9/08
G09C 1/00

(21)Application number : 09-354401
(22)Date of filing : 24.12.1997

(71)Applicant : IBM JAPAN LTD
(72)Inventor : MARUYAMA HIROSHI
TOKUYAMA TAKESHI
URAMOTO NAOHIKO

(54) CRYPTOGRAPHIC KEY DISTRIBUTION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method and a system for minimizing procedures required for updating a cryptographic key by structuring the cryptographic key into tree structure.
SOLUTION: First of all, plural keys more than the number of recipients are generated 710, and the plural keys are hierarchically arranged 720 in the form of tree structure. Next, the plural recipients are made correspondent to the keys hierarchically arranged in the form of tree structure, and the cryptographic keys of the respective recipients are generated as a key stream having keys from the root of tree structure to positions corresponding to the said recipients in the tree structure. Thus, after the cryptographic key is generated 730, the generated cryptographic key is distributed 740 to the correspondent recipient.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] A means to be the cryptographic key generative system which generates the cryptographic key for distributing to two or more addressees, and to generate two or more keys more than the number of the (a) aforementioned addressees, (b) A means to arrange said two or more keys hierarchical in the form of the tree structure, and the addressee of the (c) aforementioned plurality are matched with the key arranged hierarchical at the form of said tree structure. The cryptographic key generative system characterized by providing a means to have the key which reaches originally the location of the tree structure matched with this addressee of the tree structure in each cryptographic key of said addressee and to generate as ****.

[Claim 2] A means to be the cryptographic key distribution system which distributes a cryptographic key to two or more addressees, and to generate two or more keys more than the number of the (a) aforementioned addressees, (b) A means to arrange said two or more keys hierarchical in the form of the tree structure, and the addressee of the (c) aforementioned plurality are matched with the key arranged hierarchical at the form of said tree structure. The cryptographic key distribution system characterized by providing a means to have the key which reaches originally the location of the tree structure matched with this addressee of the tree structure in each cryptographic key of said addressee and to generate as ****, and a means to distribute the cryptographic key train by which (d) generation was carried out to said corresponding addressee.

[Claim 3] The system according to claim 2 which is a means to distribute after a means (d) to distribute said cryptographic key enciphers using said corresponding addressee's public key.

[Claim 4] The system according to claim 2 whose a means (d) to distribute said cryptographic key is a means to distribute through the Internet.

[Claim 5] The system according to claim 2 whose a means (d) to distribute said cryptographic key is a means to distribute through satellite broadcasting service.

[Claim 6] A system with said tree structure given in any [a binary tree, a ternary tree, claim 1 that is ** 4 ****, or] of 2 they are.

[Claim 7] The system according to claim 2 which changes only the key relevant to the cryptographic key which this seceder has among said two or more keys, enciphers with the key [directly under] of this key, and possesses a means to distribute the cryptographic key changed by the addressee when a seceder comes out out of said two or more addressees.

[Claim 8] A system given in claim 1 thru/or any of 2 they are. [in which a means (c) to generate said cryptographic key performs a group division for said two or more addressees with an addressee's attribute beforehand, and includes the means which matches said two or more addressees with the key arranged hierarchical at the form of said tree structure according to the relation between groups]

[Claim 9] The system according to claim 8 said whose attribute is an addressee's contract years, subscription stage, age, occupation, the address, firm, or the telephone number.

[Claim 10] The phase which is the cryptographic key generation method which generates the cryptographic key for distributing to two or more addressees, and generates two or more keys more than the number of the (a) aforementioned addressees, (b) The phase which arranges said two or more keys hierarchical in the form of the tree structure, and the addressee of the (c) aforementioned plurality are matched with the key arranged hierarchical at the form of said tree structure. The cryptographic key generation method characterized by having the phase generated as **** of having the key which reaches originally the location of the tree structure matched with this addressee of the tree structure in each cryptographic key of said addressee.

[Claim 11] The function in which is a medium including the program for generating the cryptographic key distributed to two or more addressees, and this program generates two or more keys more than the number of the (a) aforementioned addressees, (b) The function which arranges said two or more keys hierarchical in the form of the tree structure, and the addressee of the (c) aforementioned plurality are matched with the key arranged hierarchical at the form of said tree structure. The medium including a program characterized by having the function generated as ****

to have the key which reaches originally the location of the tree structure matched with this addressee of the tree structure in each cryptographic key of said addressee.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application] About the cryptographic key distribution system in broadcast mold media like the multicast in satellite broadcasting service or the Internet, this application is structuring especially a key to the tree structure, and is related with the approach and system which make min time and effort for renewal of a cryptographic key.
[0002]
[Description of the Prior Art] In satellite broadcasting service or broadcast mold media like the multicast in the Internet, when performing a user's authentication and data encryption, a key must be distributed to an addressee (subscriber). Although what is necessary is just to pass the man the key used now when an addressee newly participates, when an addressee stops participation, it is necessary to update the cryptographic key of data.
[0003] For example, a set of an addressee (subscriber) is set to S. S assumes that he is the viewer who is viewing and listening to a specific pay program. Or a set of the employee who is waiting for communication of the secrecy which is in a company is sufficient, and it is good also considering the set of a participant of the mailing list often used on the Internet as S.
[0004] Suppose that n addressees are in S. In drawing 1 , Alice, a bob, and a carol are the elements of S. Broadcaster (publisher) P enciphers and sends out Contents C. In the world of the Internet, the standardization organization IETF has proposed RFC1421 as a standardization proposal of encryption of a mailing list. This enciphers Message M with the common session key K (K (M)), and is each encryption key D1 of n persons about the K further... It enciphers by Dn (D1 (K), D2 (K), ..., Dn (K)), and it is sent out with K (M) (refer to drawing 2). An addressee decrypts the session key K with a corresponding decryption key (E1, E2, ..., En), and decrypts Message M by obtained K. When method measles is carried out and several n becomes large [an addressee], this fault that the magnitude of a key packet will become very large as compared with a message exists. For example, when a 512-bit RSA key is used for an individual key, one Di (K) becomes at least 64 bytes, and if n is 10,000, it must send out the key packet of 640KBytes about one message.
[0005] The case where how (Join/Leave Model) to distribute the common session key K using each addressee's individual key beforehand is considered is shown in drawing 3 . An individual key may be based on a common public key certificate, and may be prepared for every application. The case where the set S of an addressee has modification poses a problem here. That is, although what is necessary is to attest the user's identity using an individual key, and just to distribute K, when a new element joins S (i.e., when a new viewer participates etc.), when the element of S escapes from S, renewal of a key is serious. For example, since an audience fee was not paid even if the carol became a payday, suppose that it was going to remove from S. Since she has K, she cannot continue using the same session key. Simply, new key K' must be generated and it must be sent to the n-1 surviving addressee using each individual key. In this, when large, for example, when 100,000 viewers require n, whenever one person falls out, key delivery of 100,000 will break out.
[0006] Since there is no compatibility in the method of each company in a secret algorithm method and possession of a decoder is possession of a key, a new viewer can be made to be able to participate dynamically or the technique used for charged satellite communication etc. now cannot be made to leave temporarily conventionally. For example, the method currently used by pay-per-view etc. depends for delivery of a key on the communication link of 1 to 1 by the telephone, and has troubles, such as needing an uphill circuit and not carrying out a scale.
[0007] In addition, the approach of distributing a group key from a router is proposed as security of the multicast in the Internet. However, by this method, there is a problem on the serious security that a reliable router must be beforehand installed on a network. Moreover, this method is the security in the layer of IP, and does not guarantee the security of the end to end from application.
[0008]
[Problem(s) to be Solved by the Invention] Therefore, the technical problem which this invention tends to solve is structuring a cryptographic key to the tree structure, and is offering the approach and system which make min time and effort for renewal of a cryptographic key. Moreover, another

technical problem is offering the approach and system of cryptographic key distribution which can exhibit specification, in order to move on a known code technique. Moreover, another technical problem is the interconnectivity of each company maintaining and offering the approach and system of cryptographic key distribution which the dynamic viewer not using an uphill circuit secedes [participation and]. Moreover, however another technical problem may have a path with the problem on security in the middle of a communication link, the whole security is offering the approach and system of cryptographic key distribution which can be maintained.

[0009]

[Means for Solving the Problem] In order to solve the above-mentioned technical problem, two or more keys more than the number of addressees are generated first, and two or more keys are arranged hierarchical in the form of the tree structure. Next, it generates as **** which has the key arranged hierarchical in two or more addressees at the form of the tree structure, and the key which reaches originally the location of the tree structure matched with this addressee of the tree structure in each cryptographic key of matching and an addressee. Thus, after generating a cryptographic key, the generated cryptographic key is distributed to said corresponding addressee. In addition, in the tree structure, it has the branch derived further from each branch derived from a root (root). By the approach of this invention, there is no limitation in the number of the branches to derive. That is, the branch derived originally may be 2 and the branch derived from each of that branch may be 3. Conversely, regularity is sufficient like n ****. In drawing 4 (in the case of the form of a binary tree), K0 in the wooden root is a session key. Contents are enciphered with this session key. It is enciphered by K1 and K2, respectively, and K0 is distributed to an addressee. This is written as K1 (K0) and K2 (K0). Similarly, a key K1 is enciphered and distributed by K3 and K4. In addition, distribution of a key may be enciphered and sent with each people's public key. If it is security top insurance, it is not necessary to encipher and send with each people's public key (for example, personal delivery by the diskette is sufficient). Moreover, as a distribution means, you may distribute through the Internet, and may distribute through satellite broadcasting service. In addition, it can change suitably irrespective of the essence of this invention. Thus, by constituting, time and effort for renewal of a cryptographic key can be made into min.

[0010]

[Embodiment of the Invention] The block diagram of the cryptographic key generative system of this invention is shown in drawing 6 . Block 610 generates two or more keys more than the number of addressees first. Next, with block 620, two or more keys are arranged hierarchical in the form of the tree structure. It generates as **** which finally has the key arranged hierarchical in two or more addressees at the form of the tree structure, and the key which reaches originally the location of the tree structure matched with this addressee of the tree structure in each cryptographic key of matching and an addressee in block 630.

[0011] The block diagram of the cryptographic key distribution system of this invention is shown in drawing 7 . Although it is the same as that of a cryptographic key generative system fundamentally, block 710 generates two or more keys more than the number of addressees first. Next, with block 720, two or more keys are arranged hierarchical in the form of the tree structure. Next, it generates as **** which has the key arranged hierarchical in two or more addressees at the form of the tree structure, and the key which reaches originally the location of the tree structure matched with this addressee of the tree structure in each cryptographic key of matching and an addressee with block 730. And in the block 740 of ******, the generated cryptographic key is distributed to a corresponding addressee.

[0012]

[Example] Hereafter, the example of this invention is explained with reference to a drawing. The general-view Fig. showing one example of the hardware configuration of the cryptographic key distribution system used in this invention is shown in drawing 8 . It is the typical example of the system which distributes a cryptographic key especially through the Internet. The system 100 contains a central processing unit (CPU) 1 and memory 4. CPU1 and memory 4 are connected through the bus 2 through the hard disk drive unit 13 (or storage driving gears, such as MO, CD-ROM [23], and DVD) and the IDE controller 25 as an auxiliary storage unit. CPU1 and memory 4

are similarly connected through the bus 2 through the hard disk drive unit 30 (or storage driving gears, such as MO [28], CD-ROM [23], and DVD) and the SCSI controller 27 as an auxiliary storage unit. The floppy disk drive unit 20 is connected to the bus 2 through the floppy disk controller 19.

[0013] A floppy disk is inserted in a floppy disk drive unit 20, it can collaborate with an operating system, an instruction can be given to CPU etc., the code or data of a computer program for carrying out this invention can be recorded on this floppy disk etc. and hard disk drive unit 13 (or storages, such as MO, CD-ROM, and DVD), and ROM14, and it performs by being loaded to memory 4. The code of this computer program can be compressed, or can be divided into plurality, and can also be recorded on two or more media.

[0014] Further, a system 100 can be equipped with user interface hardware, and can have the pointing devices (the mouse, joy stick, etc.) 7 or keyboard 6 for inputting, and the display 12 for showing a user vision data. Moreover, it is possible to connect a printer through a parallel port 16 or to connect a modem through a serial port 15. It connects with a network (Internet) through a serial port 15 and a modem, or a communication adapter 18 (Ethernet and token ring card), and this system 100 can perform a communication link with the computer of others [**** / transmitting a cryptographic key] etc. Moreover, a remote transmitter-receiver machine can be connected to a serial port 15 or a parallel port 16, and data can be transmitted to it and received by infrared radiation or the electric wave (for example, transmission of the cryptographic key to an addressee etc.).

[0015] By the audio controller 21, a loudspeaker 23 receives the sound signal by which D/A (digital to analog) conversion was carried out through amplifier 22, and outputs it as voice. Moreover, the audio controller 21 carries out A/D (analog to digital) conversion of the speech information received from the microphone 24, and makes it possible to be crowded for a system in the speech information of the system exterior.

[0016] Thus, the cryptographic key generative system and cryptographic key distribution system of this invention could understand easily that it can carry out with the communication terminals containing various home electronics, such as television having the usual personal computer (PC), a workstation, Notebook PC, a palm top PC and a network computer, and a computer, the game machine which has communication facility, a telephone, FAX, a cellular phone, PHS, an electronic notebook, etc. which **********, or these combination. However, these components are not instantiation and all those components do not turn into an indispensable component of this invention.

[0017] The approach of concrete modification of a key is shown in drawing 5 . For example, when there is Alice, an audience fee is paid, and it is assumed that it became a just addressee. A server assigns a key K7 to Alice, and enciphers and sends it with the public key of Alice. Moreover, the chain of what enciphered K3 by K7, K7 [i.e.,], (K3), and a series of keys which result in the session key of the root like K3 (K1) and K1 (K0) is further sent to Alice. When the number of the whole addressees is n, the magnitude of the key chain of Alice is like log (n). Here, the case where a carol leaves the set S of a viewer by a certain reason is considered. The carol has a key called K0, K1, K4, and K10 in her key chain. Therefore, in order not to make contents access a carol from now on, the recurrence line of these keys must be carried out, and the key of a carol must be made into an invalid (it is the key which attaches X of drawing 5).

[0018] Suppose that the recurrence line of K1 was carried out, and it considered as K1'. Then, since K1 which he has becomes an invalid, Alice needs to receive K3 (K1') which enciphered new K1' by K3. Similarly, it is necessary to tell an addressee about K0' by two key delivery packets called K1' (K0') and K2 (K0'). Thereby, Alice will know K1' and K0' and can see the contents enciphered by new session key K0' from a degree. Thus, since only the key relevant to the cryptographic key which a seceder has can be changed and the changed cryptographic key can be enciphered and distributed only to the addressee corresponding to the changed key with the key [directly under] of the key when a seceder comes out out of two or more addressees according to the hierarchical key structure of this invention, time and effort for renewal of a cryptographic key can be made into min.

[0019] Next, about the redistribution effectiveness of a key, it is as follows. For example, the number of packets required for the redistribution of a key when a carol secedes is calculated. since the key which the carol had is log2 (n) individual, the number of the keys which must be generated newly is also log2 (n) (if it says strictly -- the upper method -- log2 (n) -- 1 -- small). It is necessary to encipher and send the key with the two children's key about one new key. Therefore, the number of key delivery packets required for the redistribution of a key is 2*log2 (n). If the case of r **** is generally considered, several p of a key redistribution packet will be set to p = r*logr(n) = r*log (n)/log (r). r to which n makes p min at the fixed time -- r=e -- it is (e is the bottom of a natural logarithm) -- since r is the natural number in fact -- the time of r= 3 is the optimal -- becoming -- the number of packets -- about 2.73* -- it is set to log (n). Again In the case of r= 2 If a binary tree is used, it will be actually more advantageous to use 4 **** in the case of r= 4, since the number of theory top packets is the same.

[0020] For example, it is assumed that n is broadcasting contents to 1 million, i.e., 1 million viewers. What is necessary is just to broadcast 2*log2 (106) individual, i.e., a 40 key redistribution packet, in the case of a binary tree, in order to remove one certain viewer. Since it is 2.73*log(106) =37.7 in the case of a ternary tree, if DES is used as a cipher system of a key, since one key can be sent by ID of a 64 bit + key, in ID of a key, the payload of a key delivery packet is 96 bits (12 bytes) also as 32 bits, and the whole is settled in 0.5 K bytes by this in 38 pieces.

[0021] Next, how to calculate two or more withdrawal collectively is shown below. When k persons secede collectively, it is not necessary to newly generate the key of a k*logr (n) individual. For example, it is because what is necessary is to update K0 only once. Moreover, when it turns out beforehand that several persons secede at a coincidence term, updating and the redistribution of a key when two or more withdrawal occurs can be made small by summarizing those viewers on the same possible branch (group) (when viewing and listening by the contract by the end of the month etc.). That is, an addressee's attribute performs a group division for two or more addressees beforehand, and if two or more addressees are matched with the key arranged hierarchical at the form of the tree structure according to the relation between groups, very efficient generation and distribution of a key can be performed. Moreover, contract years, a subscription stage, age, an occupation, the address, a firm, the telephone number, other individual information, etc. may be used as an addressee's attribute. It can change suitably irrespective of the essence of this invention.

[0022]

[Effect of the Invention] The distribution of an efficient cryptographic key it a specific viewer can be made to be able to participate dynamically or can be withdrawn is attained without being able to exhibit specification by this invention, in order to move on a known code technique, maintaining the interconnectivity of each company, and using an uphill circuit. Moreover, the whole security can be maintained however there may be a path with the problem on security in the middle of distribution.

[0023]